# THE BELA COMMUNITY ISSUE

## THOUGHT LEADERSHIP AND EXCELLENCE IN ACTION

**FEATURING** FLEX, stc, ALLIANZ LIFE, BAYER, & MORE

# ETHISPHERE

**GOOD. SMART. BUSINESS. PROFIT.®**

SUMMER **2022**

**PLUS!**

HOW **THE DRAWING BOARD** USES CARTOONING TO HELP ADVANCE ETHICS

MIHNEA ROTARIU

# The Top Four Indicators of Spend Risk

**By Mihnea Rotariu**

Corruption and fraud is a constant challenge for companies regardless of their size and scope. It can cost companies significant sums each year and devastate the bottom line. It can seriously hurt a company's reputation and lead to negative publicity and lowered employee morale. And most importantly, it can prompt regulatory investigations and otherwise unwanted scrutiny from law enforcement.

Understandably, effective compliance processes are a top priority for any company looking to avoid these issues. Having controls in place ensures that companies and their employees are behaving ethically. However, deciding where to start can be easier said than done. There are several factors to consider when determining what parts of a company are most prone to corruption and fraud, and it is critical to have a clear idea of where your company's most significant risks lie when developing and executing your compliance processes. Analyzing every potential indicator of spend risk in your company without context is an exercise in futility. But by focusing on these top four indicators of spend risk, your company can better position itself to prevail in its ongoing fight against corruption and fraud.

### INDICATOR #1: MARKET-BASED RISK

Understanding what segments of your company's operations pose the highest risks is foundational for every effective compliance program. There are several ways to categorize these risk areas within your company:

**Geographic Locations.** Many companies operate in multiple states, countries, or continents. Your company's compliance professionals must understand the unique challenges and regulatory expectations that come with working in various locales.

Geographic location is important on two levels: First, your company must be aware of the different compliance laws and regulatory expectations in each location. For example, if a company is headquartered in the United States but has a branch office or employees based in Germany, that company would still be obligated to implement specific due diligence procedures. For example, they would need to comply with Germany's Supply Chain Due Diligence Act when the law goes into effect in 2023.

Second, it is essential to understand that each geographic region may pose varying levels of risk and be subject to additional oversight. Jurisdictions that have AML/CFT (Anti-Money Laundering and Combating the Financing of Terrorism) deficiencies are considered high-risk and are subject to increased monitoring. Therefore, a company operating in even a limited capacity in jurisdictions such as The Bahamas, Pakistan, and Uganda, among other locations, may need to pay particular attention to risk-based policies, procedures, and practices.

**Business Entity Types.** Different industries are more susceptible to fraudulent activity. Therefore, compliance professionals need to be cognizant of the types of business entities with whom they are engaged. For example, according to Occupational Fraud 2022: A Report to the Nations, the retail industry faces a higher level of fraud than average due to inventory theft. In contrast, the healthcare, banking, and financial services industries have to contend with fraudulent billing schemes more frequently than other sectors. Understanding which businesses your company partners with and paying particular attention to those in higher-risk fields can help your company avoid unnecessary problems.

**High-Risk Company Segments.** Beyond your company's geographic footprint, consider the business operations within your organization that pose higher risks. Different departments within your company are likely to face higher odds of fraudulent activity. Examples include a companies' sales and channel partner management functions, which can be at a higher risk of corruption, bid-rigging, sanctions, or conflicts of interest, given their incentives to enable sales and the temptation to use inappropriate methods to do so.

A company's IT teams could also be considered high-risk due to the rising threats of data theft and other cybersecurity issues. Ideally, all employees within your company will receive appropriate compliance training and new monitoring tools will be implemented wherever necessary. Still, understanding which aspects of your company are most prone to risky activity can ensure that your compliance resources are focused on the correct departments.

## INDICATOR #2: DOMAIN RISK

Negligent or malicious behavior from a company's employees and the third parties with which the company engages is one of the most common indicators of spend risk. There are a handful of likely behavioral issues that compliance and audit teams should keep an eye on, including:

**Unethical Employee Actions.** Employees who perform unethically can generate significant spend-related issues for their companies. Consider employee attendance: If an employee is supposed to be working 40 hours a week but frequently clocks in or out early, they would effectively cheat their employer out of time owed. Attendance is one example of how unethical employee actions can adversely impact a company.

Another example to consider is employees' potential conflicts of interest. Conflict of interest scandals can permanently damage a company's reputation and, in the worst case, open the company up to legal scrutiny, both of which can have drastically negative impacts on a company's bottom line. For example, an opinion writer for a financial website who holds stock in a specific company may not disclose that ownership when writing about that company. If publicized, this ethical breach could cause severe reputational damage to the individual and the website. Companies need to communicate to their employees the importance of disclosing conflicts of interest and ensure that they have processes in place that enable employees to do so without fear of reprisal.

**Third-Party Behaviors.** Engaging with third parties is necessary for many companies, but doing so poses a wide variety of risks, many of which can impact a company's finances. Consider a third-party distributor that is compensated on a commission basis that is incentivized to sell more in order to earn a higher commission. An example would be if the distributor is presented with a large contract opportunity to sell to a Government Entity only if the distributor would cover the construction of a vacation home for the Government Official in charge of the Procurement Commission; if the company would go ahead with the transaction they would be exposed to a significant corruption risk of tainting all of the transactions with the Government Entity.

Third parties can pose spend risks in other ways. Third parties are susceptible to data breaches, which can pose a variety of issues for the companies with which they do business. Furthermore, the nature of their work can change over the course of their relationship with a company, which traditional due diligence processes cannot detect. For example, a third party designated as low risk during the due diligence process may have been misclassified, or the scope of their work may have changed over time. If that entity engages in risky behavior over time without oversight, it could cause the company to be adversely impacted, such as via costly legal cases or reputational damage. Traditional methods of compliance—namely, processes that can't monitor third parties after the initial due diligence process—can struggle to detect long-term wrongdoing and anomalies in a third party's behavior. However, compliance processes that feature continuous spend monitoring can help companies ensure that the third parties they are engaging are behaving ethically throughout their relationship.

## INDICATOR #3: POLICY AND TOOL RISK

Some company policies and tools can be prime targets for exploitation. These abuses do not always stem from your employees intentionally acting maliciously. For example, phishing scams, such as emails that trick employees into sharing their system passwords or otherwise sensitive information, are common cybersecurity risks that can cause myriad issues for companies. Compliance teams should ensure that their companies have safeguards in place and appropriate training courses to ensure that their colleagues are armed with the knowledge to avoid these issues. Beyond that, there are several kinds of company policies that can be indicators for spend risk:

**Automatic Approvals.** Automated approval processes, such as systems that automatically approve PTO requests and time clock systems, are prime targets for exploitation by employees seeking personal gain, cheating companies out of time and money. Be sure to implement monitoring systems to detect abnormal requests and prevent potential abuse by employees.

**Expense Policies.** Similarly, expense software is a typical company tool that can be manipulated by bad actors; an employee who submits a $10,000 meal reimbursement request is likely abusing the system. Having robust checks and monitoring in place can ensure that such activity does not go undetected.

**Gifts.** Companies need to ensure they have firm guidelines on gift-giving to avoid bribery issues, and they must effectively communicate those guidelines to employees. For example, a company's compliance system should be able to track the number and frequency of gifts given to a government official and understand the acceptable limits and norms to avoid a potential bribery scandal.

## INDICATOR #4: STATISTICAL RISK

Companies have a wealth of data spread across enterprise platforms such as Human Resources, Enterprise Resource Planning, and Travel & Entertainment systems. Compliance and audit teams must be able to locate risk indicators within their data sets, including statistical indicators of spend risk.

**Spend Anomalies.** Abnormal transaction data within a company is one of the most frequent indicators of risky activity. As previously noted, an employee who expenses a $10,000 meal is a prime example of anomalous spend activity. Companies should have clear guidelines for what kinds of transactions—and the frequency of those transactions—are considered normal and communicate that information to their employees while monitoring against those guidelines. Being transparent about the types of transactions regarded as abnormal, while automating monitoring processes, can make it easier for companies to prevent and detect anomalous activity.

In theory, detecting abnormal transactions in your data is a simple concept, but data is often siloed in disparate systems across companies. This can make it difficult to detect fraudulent activity, especially if bad actors take steps to avoid notice. If siloed data prevents your compliance and audit teams from having a holistic view of transactions, consider investing in compliance systems that can effectively pull together and contextualize siloed data sets.

**Suspicious Patterns and Trends.** One of the most important aspects of data to monitor for spend risk is suspicious patterns and trends. For example, if a company working with a third party notices a pattern of unusual payments, it could be an indicator of corrupt activity. Similarly, if an employee is filing expense reports for a $100 meal (rather than the $10,000 meal above) but doing so with an unusual frequency, that trend could also indicate potential fraudulent activity.

An effective compliance program should be able to assign risk scores to individual transactions based on a company's risk appetite. If there is a trend where transactions are continuously outside a company's threshold for acceptable risk, that aspect of the business could require additional attention.

**Completeness and Accuracy of Data.** Compliance and audit teams need to understand the completeness and accuracy of their company's data sets, as well as the limitations. While some data—such as the number of hotline reports in a given time frame or the percentage of employees who completed a training program—is not directly related to spend risk, these metrics are often used to gauge the success of a company's compliance processes, and it is important to recognize their limits. We discussed the importance of having training programs for other spend risk indicators, but just because a high percentage of employees have completed their mandatory training does not necessarily indicate that the training is being followed or understood. Similarly, a company might see a drop in year-over-year hotline reports, but that does not guarantee that less suspicious behavior is happening. It only means that less suspicious behavior is being reported. Understanding the limits of these data sets and taking steps to contextualize the data will aid compliance and audit teams in better understanding spend risk within their company.

## CONCLUSION

There are different compliance processes and tools that can help compliance and audit teams ensure that the aforementioned spend risk indicators are receiving appropriate attention. Attempting to track each of these spend risk indicators manually can be an overwhelming task, and a significant financial and manpower drain for organizations. That said, technological advancements in compliance are providing new opportunities for companies to effectively track these indicators and form more holistic views of risks across their enterprise. ■

### ABOUT THE EXPERT

**Mihnea Rotariu** *is Risk and Compliance Analytics Director with Lextegrity, a leading provider of innovative enterprise data analytics and automation technology for compliance and audit professionals at leading global companies. Mihnea has over 14 years of leadership experience in matters involving bribery and corruption, monitorships, forensic accounting, regulatory compliance, data analytics, and due diligence. His expertise spans multiple industries, including life sciences, technology, hospitality, and industrial products. If you have additional questions about methods to monitor the top spend risk indicators that companies face, reach out to Lextegrity today.*